6. Datensicherung, Datengeheimnis, Verpflichtung der Bediensteten

6.1 Datensicherung (insbesondere zu Art. 7 BayDSG)

a) Die Schulen haben technische und organisatorische Maßnahmen dafür zu treffen, dass die bei ihnen gespeicherten personenbezogenen Daten (Schülerdatei, Kollegstufendatei, Lehrerdatei, aber auch Schulkorrespondenz mit personenbezogenen Daten) vor Verlust und vor Missbrauch geschützt werden, d.h. dass

- nur Befugte personenbezogene Daten zur Kenntnis nehmen können (Vertraulichkeit),
- personenbezogene Daten vor unerkannter Verfälschung geschützt sind (Integrität),
- personenbezogene Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor zufälligem Verlust geschützt sind (Verfügbarkeit),
- die Urheberschaft übermittelter personenbezogener Daten vor deren Weiterverarbeitung festgestellt werden kann (Authentizität),
- nachträglich festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat (Revisionsfähigkeit) und
- die Verfahrensweisen bei der Verarbeitung personenbezogener Daten mit zumutbarem Aufwand nachvollzogen werden können (Transparenz).

Auf die sorgfältige Beachtung der nach Art. 7 Abs. 2 BayDSG bei automatisierten Verfahren im Einzelnen zu treffenden Sicherungsmaßnahmen werden die Schulen besonders hingewiesen. Insbesondere

- sind von personenbezogenen Daten regelmäßig Sicherungskopien anzufertigen,
- dürfen Datenträger (USB-Stick, Festplatte etc.) mit personenbezogenen Daten ausschließlich für Zwecke der Schulverwaltung verwendet werden (grundsätzlich sind Programme und Daten für den Unterricht auf gesonderten Datenträgern zu führen),
- hat die Speicherung personenbezogener Daten auf mobilen Datenträgern immer verschlüsselt zu erfolgen (Ausnahmen hiervon sind nur dann zulässig, wenn sichergestellt werden kann, dass ein unberechtigter Zugriff auf den mobilen Datenträger vollständig ausgeschlossen ist, solange dieser unverschlüsselte personenbezogene Daten enthält.),
- sind mobile Datenträger mit personenbezogenen Daten nach ihrer Verwendung jeweils wegzusperren und
- muss bei der Speicherung von personenbezogenen Daten auf Rechnern der Zugriff durch Passwörter geschützt sein, wobei ggf. abgestufte Zugriffsrechte vergeben werden sollten.

Ausführlich werden Maßnahmen der Datensicherung in der mit dem Hauptpersonalrat getroffenen Dienstvereinbarung über die Einführung und Anwendung des bayerischen Schulverwaltungsprogramms ASV in Anlage 3 „Datenschutz und Datensicherheit“ beschrieben (hierzu oben Nr. 4.2).

b) Sollen die in der Schulverwaltung eingesetzten Rechner und die Rechner für Unterrichtszwecke an ein und dasselbe Intranet der Schule angeschlossen werden, so muss in besonderer Weise sichergestellt sein, dass unautorisierten Personen ein Zugriff auf personenbezogene Daten und die zugehörenden Programme nicht möglich ist. Die Verantwortung hierfür liegt bei der Schule. Hinsichtlich des Schutzbedarfes ist es

sinnvoll, die Bereiche Verwaltung, Lehrerbereich und Schüler-/Unterrichtsbereich entweder physikalisch oder in verschiedene Teilnetze mit gesicherten Übergängen zu trennen: Durch geeignete technische Maßnahmen ist sicherzustellen, dass ein Zugriff vom Schüler-/Unterrichtsbereich aus auf Rechner in den beiden anderen Bereichen nicht möglich ist. Ein Zugriff vom Lehrerbereich auf Rechner des Verwaltungsbereiches ist auf diejenigen Dienste der Schulverwaltung einzuschränken, die zur Verwendung durch das Lehrpersonal vorgesehen sind. Die Verantwortung hierfür liegt bei der Schule.

c) Besondere Schutzmaßnahmen vor unerwünschten Zugriffen sind auch bei einem Internetzugang eines Rechners mit Zugriffsmöglichkeit auf personenbezogene Daten zu treffen. Die Verantwortung hierfür liegt bei der Schule. Geeignete Schutzmaßnahmen können beispielsweise darin bestehen, dass

– der HTTP-Datenverkehr durch einen Webfilter eingeschränkt wird,

– die nutzbaren Internetdienste dadurch eingeschränkt werden, dass vom schulseitigen Gateway (Proxy) nur unbedingt benötigte Dienste (z.B. HTTP und HTTPS für Webzugriffe) zugelassen werden,

– eine automatisierte Portfreischaltung („Plug and Play“) auf dem Router deaktiviert wird,

– ein Virenscanner den Zugriff auf Dateien und E-Mails überwacht,

– E-Mails von nicht als sicher bekannten bzw. nicht zuverlässig identifizierbaren Absendern nicht geöffnet, sondern gelöscht werden, insbesondere dann, wenn sie Anhänge enthalten,

– Verwaltungsrechner durch geeignete Authentifizierung (mindestens: Benutzername, Passwort) vor unbefugter Nutzung geschützt werden,

– die Nutzung von ActiveX-Steuerelementen, ActiveX-Plugins und „Net“-Funktionalität im Browser (Internet Explorer) grundsätzlich deaktiviert wird und

– Java und JavaScript im Browser nur dann aktiviert wird, wenn sie zur Nutzung dringend benötigter Webseiten unerlässlich ist.

Die Versendung von Schulkorrespondenz mit personenbezogenem oder sonstigem vertraulichen Inhalt mittels E-Mail ist wegen der offenen Struktur des Internets nur unter Anwendung einer Verschlüsselung zulässig, die den Schutz der Vertraulichkeit, Integrität und Authentizität ausreichend sicherstellt.

6.2 Datengeheimnis (insbesondere zu Art. 5 BayDSG)

Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Neben dem allgemeinen Datengeheimnis im BayDSG bestehen noch weitere Bestimmungen der Geheimhaltungs- und Verschwiegenheitspflichten:

– das Gebot der Amtverschwiegenheit (§ 37 BeamtStG und § 14 Abs. 1 LDO),

– das Verbot der Auskunftserteilung über Schülerinnen und Schüler an Dritte (§ 14 Abs. 4 LDO).

6.3 Verpflichtung der Bediensteten

Zusätzlich zum Amtseid ist eine gesonderte Verpflichtung auf den Datenschutz von Personen, die mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten betraut werden, nicht erforderlich.

Dessen ungeachtet empfiehlt es sich, vor Einführung eines automatisierten Verfahrens zur Verarbeitung personenbezogener Daten die damit betrauten Personen an die Wahrung des Datengeheimnisses und die Amtspflicht zur Verschwiegenheit zu erinnern.

Zu diesen Personen gehören alle Beschäftigten einer Schule, die auf gespeicherte Daten zugreifen können, z.B. Lehr- und Sekretariatskräfte, die Daten erfassen, ändern, löschen oder auswerten können, speziell also auch Lehrkräfte, die im Rahmen der Zeugniserstellung Noten an einem Computer eingeben bzw. Lehrkräfte, die Daten auf privaten Rechnern nach Nr. 4.3 verarbeiten.